МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря Сікорського»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЛАБОРАТОРНА РОБОТА №3

з дисципліни «Криптографія»

Варіант 3

Виконали:

Студенти групи ФБ-92

Шевченко Семен та

Щур Павло

Київ 2021

Завдання

Мета роботи:

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Завдання:

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда,розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

Для виконання поставлених завдань було реалізовано функцію пошуку оберненого елементу (використовує розширений алгоритм Евкліда) , функцію пошуку коренів лінійного рівняння , функцію пошуку біграм з найбільшою частотою , а також безпосередню функцію "атаки". В процесі роботи програми були сформовані всі можливі пари ключів, які були відсортовані за допомогою функції розпізнавання російської мови(в якості критерію використовується частота появи букв "а" , "о" у відкритому тексті російською мовою). В результаті було отримано можливу пару ключів (199,700). Було проведено дешифрування ШТ в результаты роботи якого було отримано змістовний текст російською мовою , а саме текст статті "Зигмунд Фрейд Достоевский и отцеубийство"

Шифрований текст, варіант 3:

кдяхэаюлтдооэтсювнкцябпосбанвооюрретлтцпвоэыохтдшылхщютзгжантзкцхнлюкднхцпвоыомхзо
тхэтоовцлшвуджозчхйбжьктибэлтцеовбдшйсвцхндншбчбоювнкцябухбюхцхнрбчэшжцюлцлхйостщ
юшужхриажгцфхзхжцитвожюфпксщхибухкйзюжмьгнхщюзншбхюэотйбавотдцюэшшылхщюабпояб
цикбкцывкцхнрбвофишбтдтхыбэляюждзютдлзщюаыпюнозоуюмхэшухэозоихщюкцзоюбзюгсвичхш
ццнщащцжхщюфмкдвощхщюйуажмздшшшкдысэтмуфьанэйсужушюстлхэдвоэомюфожхетжютдцю
гршшкдэйолнойхзозпцэкдютэтнцхыдйщюэтжцтйнбщддцывкцхнцхеоцэвбйбышкдэйюейосежхюбгц
эюубйутодткдвощхщющцяюстудвежюнхэджядшищвччощщвуной хзозпцэфтмефпшхтдпощщщыкдв
уозеойбдээзстсдоожмиврбгхнойхзозпцэцэфпэтщощюэоеохсгдюмлзсдвеньрстднтщюфпвцукеоетит
мшпнчхшцабшшлсцбухкйэыбдтджюзнхыохнхлхыбэлфошхэдохехвоубпзшбчхлыйбсуодмзеоэотэкш
фстднтщюфпкдютэтнцхыдйщюэтвцтйсдлжюасцгцеокочэкдютетэтфтщютздйирэттднттюрюецтйвмш
шзцтйищщюеокцфпжюэддйкцвмчоьйнбрбйеинухяуюгкцхнрбвотдмйбарбфшкдэтзэстсдвекдихктщ
южонжсиодгуоддйучяожстднтжхщюжощщщыгцщоцпьсждьггжнбгхгцитсдвеоонжзцэюехлцбретйхц
пвоыойбщеьжкхшцжосбанолхжжоойераннбйейсвцхндншбчбжуэтихшцвзеокэхытцажшбэйчтцпчээ
ыкояхлцюоцэвбхчшсшпвситуберончхфоыойиеыаншшвуйжышьтджфицхеогбшшанжхтдпнягвофихы
ыжжхщюзнбрщюэтудмтцпжхофгхгцзоюбрбйекцяюайбарбэтпюцпжхдйержюкшйбтдщдзщяоыбэлгт
фдэйетзэстйуэлетмюшюыхнцхтцпвотдучеощищынийькосотыкддйсуюгкцхнрбвотдьздйирэттднттю
щсзйэысесдвейхаирбтюзсжжйбщддццнтдэййбюгрбтдтхыбгцэюболхсджькдрбнхцщйеэотдднщддц
баабжукцеочтйхвюеыдйрббдфхдйыжхшшшщаышиткчсняощщуогбажбфьащелбхшзцтйищцюнхктс
дждайершецшмбзнбрфоюболохехвоаыйбсучхбзеойбйотгрбарбдкбзцбаююэттдвюкостщюьхджяор
млзсдцэфпкчшюкэфощщвуэтегрбьюетитщоойышцчшцабдншдкцжхщюцодтэоаэстжхетжютдхшкды
спнкчнжрбвотдбнкдютрртхтдетмыпюнозоуюмхэшюентлбущфскуодвюстсдвейдвугдпоябрбднтцэю
щощщтокшеронцчшццнджфитджюкцтйвмщыдйфиибшфжхмоатсбгцфпюшзцтйищгхэнкчнжрбвотд
ыгзнкдютооюывющючтсдвеэткнгстйрбмежоатсбгцфпбхьньзвоыоэозэстщоеонтмыгцндтцоохлсбан
днбрыйэвчхшцлшеочгзнжхпбхлхызцвотдтцтйвмбхохйощщжунхктсджхетжютдхшкдысжхкйгхбжйуо
лэттднттюзсзтсбшшшшушпзкцхнышбйшдшшущрбкжгажюррщазюфяшшеокояншдкцмеввнмжхетж
ютдхшкдысбхьнэлжхэоейфитдтхыбэлтднтзбшшернбйедшзцтйищцюджфицхяберстфпвоэуажкбруат
еоахщюмхэшухжцлжрбгхкйпнвопюшцлшшшэтихшцтжбфоилсуюыяшшеокояащелбучиххцхнрбвонс
тднбансюуйщодэнтихыбюешюыхнцхтцпетщцжжйбвотддцитвожюшцбдшшсущантсофогбсурржцзо
жюдюяюэоддтххгнхщюжбзнкофтждждцжжйбвотдромхжюгбгцлхкссдкйрретфпасйотдухвцщоыояоет
ктйхэдетэьвугцышшсажкбгцфпкйщеьжкхшццнйовныжрбвоенэизнеожретмхщюдшшшухсугждннььг
ррщюцйюгдткуюгаюетмютхыойотднтыбгцэюжхюбвукдвощхщюдшчобхдбдшжуьжгажюпнньхыохзй
зцвоыыйбсунбцюэозоихщюмолесбсуммяюепдэйхсбрбвогьвугцышшсажкбгцфпюшшшетждрсэтзэст
удобжьлзтцлхыбвхкйсудйхюххыокйзювнфирбюлчозтлхтбйбьзньйбйужькюдурбщдфхгжеыникоьбг
цэюйбрбднтцэюлжгажющощщкющанмжюйорршхжщюфмэощняюабгххсййбргшзцтйищцюжхинфи
ывйугнрцнмттетяюххаюитйхкчэоэтесшцраирушжцчэмюсуажандйщеябруеыохпыыжкьцчгдзюшхыб
фшвуйжышэшзцтйищцювснхеокшзожххцлжкбьхвцньйбгцшхщстхвюфпгдхыпюнонбажщдьзкцсюмо
тэшцитжюэюшхыбмкэюцнлхщюцнжхвцлшжьгцвужхщюююетнобюхнщютшкчншкчбохсжхыйбркюю
ышдчхагьхыовцислтсдшшетзэстйуолсылжэыпюшбхфньхытцодгжабйбхфйужцбретщюудшшйсвишд
беьжрбйеооьжзцэющоеоаэзбвмнищдвеетштехлцбретйхцпетмыпюеюмхэшюеыюлбссэтфтыбрудэщ
хжхтцмхрыонцчшццнйиеыанвущоьылхнцэыгцлхэцхнйедэйхсбрбйежхетжютддшкдысводэяеьжкхш
цбдлзеоушйбяхщоцщанкдьгнхтдьжрбгхчощщвуфтоознончххнетщхяеэотдщеыбухшхтдмкеокдьгнхт
дьжрбгхооюывющючтсдвеетнюяевокйфитдднсесдчобоэнжхфочовсрюхцитцщвчкйкдпнгцеопвхчгц
итцпвохсчонххгнбвчетщхыошучберончхпджьмтждкюхцитцщвчетнюицтхшмююкйеытцончхшхжбзц
лхгбущдйнищдгждцщоыоьжйещюаблюстюбхлнююямбощцюкцяюкдлщцэьцайанетпюцптдтхнгкце
оубхфкцтхшммыдйрбсучхеоябньмкэюэтмхтдстпнньпоябсфрбцюдесбанднбрщюэтсдатлцпнвотдхш
кдэйолэтзйеретхжвгажщаиашдбншдкцжхыболиндйчетдажгцситцэюмхэшсущцитвожюшцшуерюмт
цшцсюпдухтдбнгцвотхинухчгрбтдтхыбхызцпюибруибхфйуцнбрщюэтсдбоцпштмыкдохьбгцфпибшш
ернбцюйекдлттдяогичхшцбалшшшитщооозннтюыэйсгрбгхшсшпцэкдлттдкгрбвмнищдрианлххнэйр
бгхщгкцеощофоойэврбцюсбсуиндйчечолбнбгхжючээтвиюеэтнтцнсесдветхшпоосбанкцоохлэттднтт
юхлдшшшитщостжошсзхтдьжрбгхмюлбпзажкбжьхызцпюибжьпоябсфрбйещощщкюшсшпдтушйбях
щоцщаняюепмтцпжхофюекйухощйекдютвоэуажкбвхцнлхщюмыкотцноуеьюэывюаоэумйаннбцючо

тхтдэиыжюбдыюмнищдкбуофюьтыбвхпикцутвоэуажкбвхетшхзхжхриажгцсстднбанщдюйерййнбьз
рбйешхвимбсурржутзчхшцвзеоетйаыжтфюекоцппикцбнщожхвбвущджьэывюфюнэстсдвеатлцпнчэ
склхшхэджудэйхсбрбвочгрбтдтхыбгцэюгхзхэтнцислтжбэлгтфдэйсуьхцретмхщюбеьжкхшцтжпнгсшт
ввюлтднтнойхтюмихлтджюйхцпвотдяочоехыбйбзцлждцхнрбчэскеокдвопюшцлшйотдухвцщохсгтф
дньзюэшкчаюйхцпвоыойсвцхндншблйднвоэтсючтсоеютдэшжьпоойерягррщюкэиннисуюхыогцщар
бвоуйщодэнтихыбвучшвуэожхэдюгрбтдтхыбгцэюйотдухвцщоыофоюбпокйфигжщддцлхксввсущант
софочоехыбгцлжкбюешюыхнцхтцпетмыохцйзцэозоихыбгцфптцэочоьбгцфпчочобоацлжолфтьюжт
фпвекдфтжюпюфотдяобзохвнщзтлвошскоооыокдютждкдртнтфддйшюыхнцхтцпвотдсуыищаднсей
узйнбьхдретыбрущоьыйбрбитшхыошсзхтдстнтыбюлпюьыеоьывюатошанкудйэюфоюбэйзцкуодвюс
тфпэтщоеовикцхнлхщюкцооньщечощщвуйоюсзхыбухушпзкцхнрбшшернбйечотдэййбсцтхшмбдпрв
мкдгжэащдрощщсиюасцитфпкдьоицжувундэыдйлдюойхфбпойхнудйхнэлщащзчэяуемнбррмютдд
йьзкцсюбцсучдвуандшеохсихйхбхщпйхлеэапнчхеойхшисеетщхыощцсучдвукудйэюцнсесдверианлх
хнэйрбгхыянбитйюсуюгэшжььггжнбйеяогбанохшхыбвуерюмтцшцсюьыгцохэцхнвуетэтфтщюбдухтд
дцситцэюмхэшсурианлххнэйрбгхфодтююиндйчехьнтудкоцпкдютэиажтфзнщазхфоябсфрбгхшхвияж
ьзвотдучяоехфдвукдюткйтцюмнтжхщюгхыочонххгнбйебхохвжанкдвощхщюйувгксююиндйчевостю
юхцяхщюкоушнбднеокоацяхжхитсюоюйянбэюцпчэдйщтощцюйиеыаншшвуйжышьтфоэсцркьзозбн
дфхджэихлтджюйхцпвотдкбфичхэюенмтцпжхофйуфюьювортнтфддйкдютгцитсдвейхагкцжуружхео
гсослфчхшцщцыомтмюитсюфоойервукйниыжзтсдгцитстфпвешбрбднтцфпйотдухвцщоыощощщюгг
нбгхкудйэюждвудрзохскдыстднбанщдвехызцчэшхджщдшшгхдэйхсбрбчэвггжнбйегцывкцхнсеудве
етнхлхгтэдерйетдажбйщтцпвотдучвцйудйпрэвщдшдэыдйут

Розшифрований текст, варіант 2. Ключ – a = 199, b = 700

отцеубийствокакизвестноосновноеиизначалыноягрестнглениечеловечестваиотделыноцочеловека
вовсякомслучаеонфплавньйисточникчувствавиньнеизвестноединственньйлиисследованиямнеуда
лосыещеустановитыдушевноепроисхыждениевиньипотребностиискнгленияноотнюдынесзществе
нноединствебньйлиэтоисточнидгсихологическоеположениесложноинуждаетсявобясненияхотнош
ениемалычикакоткукакмвповоримамбивалентнопомимоненавистииззакоторойхотелосыбьотцака
ксигерникаустранитысзществуетобьчноншкотораядолянежностикнемуобаотношениясливаютсяви
дентификациюсотцомхотелосыбьзанятыместоотцщготомучтоонвьзьваетвосхищениехотелосыбьбь
тыканонипотомучтохочетсялпоустранитывсеэтонаталкиваетсянакрупноепрягятствиевигределебнь
ймоментребенокначинаемгониматычтопопьткаустранитыотцакаксигерникавстретилабьсосторонь
отцанаказаниечерезкастрациюизстрахакастрациитоестывинтересахсовранениясвоеймужественно
стиребенокотказьваетсяотжеланияобладатыматерыюиотустраненияотцщгосколыцуэтыжеланиеос
таетсявобластибессознателыноцооноояоляетсяосновойдляобразованиячувствавиньнамкажетсячто
мьигисалинормалыньягроцессьобьчнуюсудыбутакназьваемоцоэдвговакомплшкюаследуетоднако
внестиважноедигвлнениевозникаютдалынейшиеосложненияеслиуребенкасилынееразвитконстит
уциобньйфакторназьваемьйнамибиеексуалыностыютогдщгодщпрозогготеримужественностфчере
зкастрациюукрягляетсятенденцияуклонитысявсторонуженствебностиболеетфпотенденцияпостави
тысебянаместоматеривгеренятыеервлыкакобшкталюбвиотцаодналишзбоязныкастрацииделаетэту
развязкуневозможнойребенодгонимаетчтоондолженвзятынасебяикастрированисеслионхочетбьт
ылюбимьмотцомкакженжинатакобршкаютсянавьтеснениеобапорьваненавистыкоткуивлюбленнос
тывотцаизвестнашгсихологическаяразницаусматриваетсявтомчтоотненавистикотцуотказьваютсявс
ледствиестрахщгередвнешнейопасностыюкастрациейвлюбленностожевотцаволгринимаетсякаквн
утренняяопасностыпеэвфчноцопозьвакоторашгосутисвоейсновавозхращаетсяктойжевнешнейигас
ностистрахпередотцамделаетненавистыкоткунеприемлемойкастрацияужаснакаквкачествшкарьта
киценьлюбвиизобоихфакторовввьтесняющихненавистыкоткупеэвьйнепосредствебньйстрахнаказан
ияикастрациисследуетназватынормалыньмпатогеническоеусилениепривноситсякаккажетсялишыд
ругиафакторомбоязныюженственнойустановкиярковьражебнаябиеексуалынаясклонностыстанови
тсятакимобразомоднимизусловийилиподтвержденийневрозаэтусклонностыочевидносследуетприз
натыиудостоевскоцоионалатентнаепомосшксуалыностыпрояоляетсявдозввленномвидевтомзначе
ниикакоеимелавлпыжизнидружбасмужчинамивецодострабностинежномотношениихсоперникам
олюбвиивлпигрекраснотгониманииположенийобяснимьхлишывьтесненноппомосшксуалыностыю

какнаэтоуказьваютмнфпочислебньепримерьизецопроизведенийсожалеюнонфчлпонемфпуизмен
итыеелвгодронностионенавистиилюбвикотцуиобихвидоизмененияхподвлияниемугрозькастрации
несведзщемувпсихоанализечитателюпокажутсябезвкусньмиималовероятньмвгреюгвлжпаючтоим
ебнокомплшкскастрациибудетотклоненсилынсевслпоносмеюуверитычтигсихоаналитфческийопьт
ставитимебноэтиявленияявневсякфпосомнения инаходитвнихключклюбомунехрозуилгьтаемжсецо
вслучаетакназьваемойцгилягсиинашлпигисателянонашемусознаниютакчуждьтеяоленияваоластик
оторьхнаходитсянашабессознателынашгсихическаящизныуказабньмвьшенеисчекгьваютсявэдвгов
омкотглексягоследствиявьтеснения ненавистикоткуновьмяоляетсяточтовконцеконцовотыждестол
ениесотцомзавоевьваетвнашемяпостоябноеместоэтоотыждестолениеволгринимаетсянашимяноп
редставляетсобойвнемособуюинстанциюпротивостоящуюосталыномусодержаниюнашецоямьназ
ьваемтфпдаэтуинстанциюнашимсверхяипрвгисьваемейнаследницеродителыскоцоолияниянаива
жнейшиефункцииеслиотецбьчсуровнасилыственжестокнашесверхшгеренимаетотнлпоэтикачества
ивлпоотношениикясновавозникаетпассивностыкоторойкакразнадлежалобьбьтывьтеснебнойсверх
ясталосадистическимястановитсямазохистскимтоестывосновесвоейженствебнигассивньмвнашемя
возникаетболышашготренностывнаказаниияотчастиотдаетсебякактаковоевралгоряжениесудыбь
отчастиженаходитудовлетворениевжестокомобращениисниМсверхясознаниевинькаждаякараявля
етсяведывосновесвоейкастрациейикактаковаяосущестолениемизначалынфпигассивнфпоотношен
иякотцуисудыбавконцеконцовлишыдалынейшаяпроекцияотцанормалыньеявленишгроисходяжия
гриформированиисовестидвлжнхгоходитынаопиюабньездесыанормалыньенамещенеудалосыуст
ановитыразгранфчениямеждунимизамечаетсячтонаибвлышаяролыздесывконечномитфпягрипись
ваетсяпассивньмэлементамвьтесненнойженствебностиищекакслучайньйфакторимсетзначениеяо
ляетсяливнушающийстрахотецивдействителыностиособебнонасилыственньмэтоотносится кдостое
вскомуфактлпоисключителыноцочувствавиньравнокакимазохистскфпообразажизнимьсводимкец
оособенноярковьражебномукомпонентуженствебностидостоевскоцоможноопределитысследующ
имобразомособебносилынаябиеексуалынашгредрасположебностыиспосонностысособойсилойза
жищатысяотзависимостиотчрезвьчайносуровоцоотцаэтотхарактербиеексуалыностимпдобавляемк
рансеузнабньмкотгонентамецосуществарабнийситготгрипадковсмертиможнорассматриватыкако
тождествлениесволпоясотцомдопущебноевкачественаказаниясостороньсверхятьзахотелубитыотц
адабьстатыотгомсамомутягерытьотецноотецмертвьйобьчньймеханизмистерфческихсимптомовик
томужетеперытебяубиваетотецдлянашецоясимптомсмертиявляетсяудовлетворениеафантазииму
жскфпыжеланияиодновремебномазохистскитгосредствомнаказаниятоестысадистическимудовлет
ворениемобаяисверхяопраютролыотцаидалышевобщемотношениемеждулфчностыюиобектомот
цаприсохраненииецосодержанияперешловотношениемеждуяисверхяноваяинсценировканавторо
йсценетакиеинфантилыньереакцииэдвговакомплшкюамогутзжплохнутыеслидействителыностыне
даетимвдалынейшемпижинохарактеротцаостаетсятемжесамьмнетонухудшаетсясцодамитакимоб
разомпродвлжаетоставатысяиненавистыдостоевскоцокотцужеланиесмертиэтомузломуоткустанов
итсяигасньмеслитакиевьтесненньежеланияосзществляютсянаделефантазиясталареалыностыювсе
мерьзащитьтягерыа